May 23, 2000

INSPECTOR GENERAL REGULATION 5200.2-R

SUBJECT: Personnel Security Program

References: See Appendix A.

A. Purpose. This Regulation establishes responsibilities, policy and procedures for the administration of the Personnel Security Program of the Office of the Inspector General, Department of Defense (OIG, DoD), and implements references a and b.

B. Cancellation. This Regulation supersedes IGDR 5200.2, *Personnel Security Program*, February 12, 1990.

C. Applicability. This Regulation applies to the Offices of the Inspector General; the Deputy Inspector General; the Assistant Inspectors General; Director, Administration and Information Management; Director, Departmental Inquiries; and Director, Intelligence Review; and the Office of the General Counsel (Inspector General), which is provided support by the OIG, DoD. For purposes of this Instruction, these organizations are referred to collectively as OIG components.

D. Definitions

1. **Collateral Information.** All national security information classified Confidential, Secret or Top Secret under the provisions of the DoD 5200.1-R, "DoD Information Security Program Regulation" (reference c).

2. **Interim Security Clearance.** A security clearance granted on a temporary basis pending the completion of all investigative requirements.

3. **Personnel Security Clearance Determination.** A determination concerning an individual's eligibility for employment or retention in a sensitive position and eligibility for access to classified and/or sensitive unclassified information. The determination is based on an assessment of all available information, favorable and unfavorable, with emphasis on the seriousness, recency, frequency and motivation for the individual's conduct.

4. **Sensitive Position.** Any position within the OIG, DoD, in which the occupant could bring about, by virtue of the nature of the position, a materially adverse affect on the national security. All civilian positions are special-sensitive, critical-sensitive, noncritical-sensitive or nonsensitive, as described in paragraph H of this Regulation.

5. **Sensitive Unclassified Information.** Any information that, if lost, misused, disclosed or destroyed, could adversely affect the national interest or the conduct of OIG, DoD, operations or Federal programs, or the privacy to which individuals are entitled under Section 552a of title 5, United States Code, The Privacy Act (reference d). Typical types of data that are considered sensitive are "For Official Use Only," proprietary, financial and mission critical information.

6. **Suitability Determination**. A requirement for Federal employment that refers to a person's character or conduct that relates to the efficiency of the service. If such character or conduct jeopardizes the accomplishment of the OIG, DoD, mission or may prevent effective service in a specific position, the employee or applicant may be found unsuitable. Suitability determinations are

made by the Director, Personnel and Security Directorate (PSD), Office of Administration and Information Management (OA&IM), and are distinct from personnel security clearance determinations.

E. Delegated Authorities

1. **Washington Headquarters Services Consolidated Adjudication Facility (WHS CAF).** The WHS CAF is the delegated authority in deciding personnel security clearance determinations for OIG, DoD, civilian employees and/or applicants. The parent Service CAF of the military member assigned to the OIG, DoD, is the delegated authority for personnel security clearance determinations.

2. **Washington Headquarters Services Clearance Appeals Board (WHS CAB).** The WHS CAB is the delegated authority in deciding appeals of unfavorable personnel security determinations made by the WHS CAF. The WHS CAB consists of a president, who is a permanent member of the WHS CAB, and two ad hoc members. A senior OIG, DoD, official serves as an ad hoc member of the WHS CAB to ensure that OIG, DoD-unique programmatic and management interests are represented during WHS CAB deliberations on OIG, DoD, civilian employees and/or applicants.

3. **Defense Intelligence Agency Central Clearance Facility (DIA CAF).** The DIA CAF is the delegated authority in deciding OIG, DoD, military and civilian personnel eligibility determinations for access to Sensitive Compartmented Information (SCI).

F. Policy. The OIG, DoD, Personnel Security Program is established by this Regulation. Familiarity and compliance with the Personnel Security Program is mandatory for all OIG personnel. The Security Division, PSD, OA&IM, is the delegated authority for the Personnel Security Program.

G. Responsibilities

1. The **Inspector General** will maintain oversight of the Personnel Security Program and ensure OIG components comply with this Regulation.

2. The **Director, OA&IM,** will manage and control the overall program in accordance with this Regulation.

3. The **Director, PSD, OA&IM,** will:

(a) Administer the program and provide general policy and technical guidance for the Personnel Security Program through the Chief, Security Division, PSD, OA&IM.

(b) Exercise the authority to suspend an employee's access to classified and sensitive unclassified information and assignment to sensitive duties when made aware of issues that warrant further clarification and adjudication regarding an employee's judgment, reliability and/or trustworthiness.

(c) Exercise the authority to notify an employee of the intent to deny or revoke a security clearance and eligibility for employment in a sensitive position.

4. The **Chief, Security Division, PSD, OA&IM,** will:

(a) Provide personnel security services within the OIG, DoD, in accordance with references e through l.

(b) Conduct Preappointment Security Checks in accordance with paragraph K.4. of this Regulation.

(c) Serve as the OIG, DoD, single point of contact to the WHS CAF for processing personnel security clearance eligibility determinations for assignment to sensitive OIG, DoD, positions and/or access to classified information.

(d) Serve as the OIG, DoD, single point of contact to the DIA CAF for processing personnel security clearance eligibility determinations for access to SCI.

(e) Initiate investigations on OIG, DoD, personnel for continued assignment to positions requiring access to classified material or when adverse or questionable information becomes known.

(f) Implement and monitor the Periodic Reinvestigation Program.

(g) Ensure that positions are designated in accordance with paragraph H of this Regulation.

(h) Request appropriate security clearances.

(i) Issue interim Secret security clearances.

(j) Recommend processing an exception memorandum to the OIG component.

(k) Suspend an employee's access to classified and sensitive unclassified information when adverse and/or questionable information becomes known and warrants clarification and/or adjudication regarding an employee's judgment, reliability and/or trustworthiness.

(l) Conduct requisite briefings and debriefings for individuals in accordance with paragraph P of this Regulation.

(m) Evaluate, for possible referral to the appropriate counterintelligence agency, written reports submitted by individuals who have reported contact with foreign nationals as required by paragraph P.3. of this Regulation.

(n) Certify security clearance data to industrial firms and Federal agencies for official visits.

(o) Control the issuance of DoD building passes.

(p) Take such other actions as are appropriate for the efficient and effective functioning of the Personnel Security Program in the OIG, DoD.

5. The **OIG Component Heads** will:

(a) Determine and document the position sensitivity level for all civilian positions within their component in accordance with references e through l.

(b) Determine the level of access to classified information required and forward a request, in writing, to the Security Division, PSD, OAIG-A&IM, that such clearance/access be granted.

(c) Ensure that all personnel within their component are aware of the provisions of this Regulation.

H. Designation of Position Sensitivity

1. Position sensitivity designations will be made in accordance with references a, b and Appendix A, and are designated based on the needs of the position in one of the following sensitivity levels:

(a) Special-sensitive

(b) Critical-sensitive

(c) Non-critical-sensitive

(d) Non-sensitive

2. The criteria for designating each position sensitivity level and its investigative requirements are specified as follows:

(a) Special-sensitive

(l) Access to SCI.

(2) Access to the Single Integrated Operation Plan - Extremely Sensitive Information (SIOP-ESI).

(3) Category One and Category A Presidential Support activities.

(4) Special Access Programs requiring a Single Scope Background Investigation (SSBI) when designated by the Assistant Secretary of Defense (Command, Control, Communications and Intelligence).

(5) Level 4 automated data processing (ADP) positions. See DoD Directive 5200.28, "Security Requirements for Automated Information Systems" (reference j).

(6) Positions designated as special-sensitive require an SSBI, which must be favorably adjudicated before appointment. This requirement cannot be waived. The investigation is updated every 5 years with a periodic reinvestigation.

(b) Critical-sensitive

(1) Access to Top Secret information.

(2) Development or approval of plans, policies or programs that affect the overall operations of the DoD.

(3) Development or approval of war plans, plans or particulars of future major or special operations of war, or critical and extremely important items of war.

(4) Investigative and certain investigative support duties, the issuance of personnel security clearances or access authorizations or duty on personnel security boards.

(5) Fiduciary, public contact or other duties that demand the highest degree of public trust.

(6) Duties involving access to approved Special Access Programs not requiring access to SCI.

(7) Level 3 ADP positions. See reference j.

(8) Critical-sensitive positions require a favorably adjudicated SSBI initiated before appointment. In an emergency situation, the completed SSBI requirement may be waived, in accordance with paragraph J of this Regulation, if the OIG Component Head finds the delay in appointment would be harmful to national security and states, in writing, that the overall effectiveness of the mission of the organization would be affected. However, the position may only be filled when there is a valid, favorable National Agency Check (NAC) or National Agency Check with Inquiries (NACI) and the SSBI has been initiated. The SSBI is updated every 5 years with a periodic reinvestigation.

(c) Non-critical-sensitive

(1) Access to Secret, Confidential, "For Official Use Only," "Privacy Act" and sensitive unclassified information.

(2) Security police/provost marshal-type duties involving law enforcement and security duties concerning the protection and safeguarding of OIG, DoD personnel and property.

(3) Level 2 ADP positions. See reference j.

(4) Duties involving the design, operation or maintenance of intrusion detection systems deployed to safeguard DoD personnel and property.

(5) Duties involving access to an approved Special Access Program not requiring access to SCI or Top Secret information.

(6) Non-critical-sensitive positions require a favorably adjudicated NACI before appointment. In an emergency situation, the completed NACI requirement may be waived, in accordance with paragraph J of this Regulation if the OIG Component Head finds that the delay in appointment would be harmful to national security and states, in writing, that the overall effectiveness of the mission of the organization would be affected. However, the position may only be filled after the NACI has been initiated. Individuals with a security clearance and current access to Secret information shall receive a periodic reinvestigation for Secret access at 10-year intervals.

(d) Non-sensitive

(1) All other positions not meeting the criteria for special-sensitive, critical-sensitive or non-critical-sensitive shall be designated as non-sensitive.

(2) To occupy a non-sensitive position, a NACI must be favorably completed on a post-appointment basis.

I. Limitations/Restrictions

1. The OIG Component Heads have the authority to designate the security sensitivity of each position within their component. The designations will be based on the specific duties of each position and/or access to classified and/or sensitive unclassified information. Encompassed within

that authority is the responsibility of each OIG component to hold sensitive positions to a minimum consistent with mission requirements. The designated position sensitivity level is recorded on Optional Form 8 (OP 8), "Position Description."

2. Management officials will ensure that all requests to recruit for vacant OIG, DoD, positions are forwarded to the Personnel Operations Division, PSD, OA&IM, via a Standard Form 52 (SF 52), "Request for Personnel Action," to include a current and accurate position description with the accompanying OP 8. Vacancy announcements will inform applicants of the security investigative requirements of the position, and that an unfavorable personnel security determination could make the individual ineligible to occupy the position.

3. Changes in an employee's position description that affect position sensitivity will be coordinated before making the revised position description effective through the Security Division and the Personnel Operations Division, PSD, OA&IM. The Security Division will ensure that investigative requirements have been met and the individual has been found eligible for duties at the new sensitivity level, in accordance with paragraph K.4. of this Regulation. The OIG Component Head will request the change in position sensitivity in writing. The request must state the reason for the change and shall be submitted, along with the revised position description, OP 8 and SF 52.

4. Position sensitivity levels shall be reviewed annually, but not later than March 30 of each year, to ensure accuracy. Changes will only be made and approved on a case-by-case basis. Improper designations should be avoided. Designations that are too high impose costly and time-consuming investigative requirements and needlessly delay the appointment of the applicant and accomplishment of the duties of the position. Designations that are too low compromise national security by employing applicants in positions where they could cause harm to the Nation.

5. Positions shall not be temporarily redesignated to a lesser degree of sensitivity to bypass investigative requirements to fill a position more rapidly. The Security Division, PSD, OA&IM, will review all requests for redesignation of position sensitivity to ensure compliance of those stated limitations and restrictions. The Security Division will contact the OIG component representative and the Personnel Operations Division, PSD, OA&IM, for necessary corrective action.

J. Exception Memorandum

1. The DoD has established specific investigative requirements for sensitive positions. In an emergency situation, the OIG Component Heads, with written coordination from the Security Division, may approve an exception to the required preemployment investigative requirements for employment in and/or assignment to critical-sensitive and non-critical-sensitive positions. The exception memorandum must include a statement that the delay in appointment would be harmful to national security and that the action is necessary for the accomplishment of an OIG, DoD mission. Rationale supporting that determination must also be included.

2. Although requirements may be waived to place the applicant/employee in a sensitive position pending an investigation and adjudication of that investigation, preemployment checks, as identified in paragraph K of this Regulation, and minimum investigative requirements must be favorably completed before an exception can be approved. (Note: The exception memorandum is for employment purposes only and does not constitute the issuance of a security clearance.) The investigation will continue and will be adjudicated on completion.

3. Additionally, the OIG component will be notified of known potentially disqualifying information concerning the nominee before an exception to the investigative requirements is processed. The OIG Component Head will review the information and notify the Security Division of his/her intention to waive the investigative requirements of the position or remove the applicant's name from the "leading candidate" status. While it is the prerogative of an OIG Component Head to

submit an exception memorandum, the issuance of the security clearance or SCI eligibility determination remains the responsibility of the delegated adjudicative authority.

4. The approved exception memorandum will be returned to the Security Division, PSD, OA&IM, for appropriate record keeping.

5. An exception to preemployment investigative requirements is not required when an employee's position is being upgraded to a higher sensitivity; however, the necessary investigation must be conducted and favorably adjudicated.

K. Preemployment Checks. Employment in an OIG, DoD, sensitive position is a shared responsibility of the OIG component and the PSD, OA&IM. As a minimum, for employment in a sensitive position, the following preemployment checks are required on an applicant identified as the "leading candidate" and will be completed by the office indicated:

1. **Hiring Officials/Supervisors**

(a) Ensure position sensitivity is current and accurate before requesting personnel actions to recruit and/or changes in position sensitivity level designations.

(b) Advise the Personnel Operations Division, PSD, OA&IM, in writing, whenever the sensitivity of any position changes.

(c) Review the SF 171 and/or equivalent application resume for suitability issues, accuracy and qualifications.

(d) Conduct reference checks with the current and most recent former supervisors. Document information that is relative to the applicant's suitability for employment and provide written results to the Personnel Operations Division.

2. **Employee Relations Division, PSD, OA&IM**

(a) Schedule the "leading candidate" for a preappointment drug screening test at an approved medical facility located closest to the applicant's location.

(b) Notify the Personnel Operations Division, PSD, OA&IM, of the results of the test. If the applicant's test result is negative for illegal drug use, the employment process continues. If the applicant's test result is positive for illegal drug use and/or the applicant declines the opportunity to be tested, the OIG component will be notified and the employment process ends.

3. **Personnel Operations Division, PSD, OA&IM**

(a) Provide advice and assistance to supervisors on designation of position sensitivity in accordance with references e through l and this Regulation before recruitment or other personnel actions.

(b) Ensure the designated position sensitivity level is recorded on the OF 8 and the SF 52 before recruitment or any other requests for personnel actions are forwarded to the Security Division, PSD, OA&IM, for processing.

(c) Verify U.S. citizenship.

(d) Conduct inquiries with the losing agency, including review of the Official Personnel Folder, to ascertain whether there is adverse suitability information and the level of security clearance issued, if any.

(e) Inform the hiring official/supervisors and the Security Division of its findings.

(f) Ensure required documentation is maintained appropriately.

(g) Process all requests of recruitment, changes in position sensitivity levels and positions through the Security Division, PSD, OA&IM, before commitment.

4. **Security Division, PSD, OA&IM**

(a) Review all data provided by the Personnel Operations Division to determine security eligibility.

(b) Review the position sensitivity determination and ensure that documentation is maintained in the appropriate security files, to include the OP 8, the SF 52 and the Notification of Incoming Personnel.

(c) Verify prior personnel security investigation and clearance are current and meet regulatory standards.

(d) Request the individual to complete a SF 86, "Questionnaire for National Security Position," when required.

(e) Advise the OIG component of potentially disqualifying information.

(f) Initiate an SSBI and/or NACI, as needed.

(g) Adjudicate applicant cases for the issuance of an interim Secret clearance and notify the WHS CAF to update the Defense Clearance and Investigative Index (DCII).

(h) Request the WHS CAF issue a personnel security clearance or,

(i) Request the DIA CAF make a determination for SCI eligibility.

L. Personnel Security Adjudication

1. The WHS CAF is responsible for personnel security clearance adjudications for OIG, DoD, personnel assigned to, or applicants for, sensitive positions. All pertinent personnel security information and reports of investigation concerning OIG, DoD, employees and/or applicants are furnished directly to the WHS CAF by the Security Division for the following purposes:

(a) To ensure that the investigative requirements are met. If the investigative requirements are not met, the Security Division will take action to request an appropriate investigation to meet the requirements.

(b) To assess unfavorable information and to apply security standards, as contained in Appendix B of this Regulation, and in compliance with Appendix C of this Regulation.

(c) To address concerns regarding an employee's judgment, reliability and/or trustworthiness.

2. If the available personnel security information is determined to be favorable, eligibility for employment in a sensitive position and/or continued employment in a sensitive position will be authorized, and the WHS CAF will issue a certificate of clearance. The certificate of clearance will be forwarded to the Security Division for inclusion in the Personnel Security Folder, the Official Personnel Folder and notification to the employee through the OIG component. If the individual is an applicant, the Personnel Operations Division, PSD, OA&IM, will maintain the Official Personnel Folder copy pending the applicant's entrance on duty.

3. If available personnel security information is determined to be unfavorable, the following procedures apply:

(a) Pre-Appointment (Applicant)

(1) Before determining an applicant as a "leading candidate" and/or extending a tentative offer, the Personnel Operations Division, PSD, OA&IM, and appropriate management officials will determine whether an applicant is suitable for employment or whether action to discontinue the employment process is warranted. The Personnel Operations Division, PSD, OA&IM, will notify the Security Division of any unfavorable suitability determinations for cancellation of any pending adjudicative and/or investigative actions.

(2) If a determination is made to discontinue the employment process, the Personnel Operations Division, PSD, OAIM, will notify the applicant of that decision. The applicant will be afforded all procedural rights in accordance with the provisions of reference c, i.e., the right to appeal the decision to the Merit Systems Protection Board.

(3) If a favorable suitability determination is made, the Security Division will forward a request for a personnel security determination and the issuance of a personnel security clearance to the appropriate adjudicative authority.

(4) If the WHS CAF personnel security determination is favorable, the WHS CAF will issue a security clearance and forward the certificate of clearance to the Security Division for dissemination.

(5) If an unfavorable personnel security determination is made by the WHS CAF, the following actions will be taken:

a The WHS CAF will issue a Statement of Reasons (SOR) through the Security Division, PSD, OA&IM, informing the applicant of the tentative determination to deny eligibility for employment to a sensitive position and a security clearance. The SOR will:

1 Include a written statement of the basis for the unfavorable personnel security determination.

2 Advise the applicant that he/she may reply in writing and may provide documentary evidence and/or affidavits in support of the reply.

3 Inform the applicant that he/she may request the investigative file by contacting the agency that conducted the investigation and provide the name and address of the investigative agency.

4 Afford the applicant 30 days, from the date of receipt, to submit a written reply to the WHS CAF through the Security Division.

5 Provide the applicant instructions for responding to the SOR (see Appendix D, "Instructions for Responding to a Statement of Reasons").

b The SOR will be mailed to the applicant by registered mail, with a copy furnished to the OIG component. The applicant will be requested to sign the Acknowledgment of Receipt. A copy of the signed Acknowledgment must be returned to the WHS CAF through the Security Division to establish a 30-day suspense for the applicant's reply. At the expiration of the 30-day response period, the WHS CAF will consider all relevant information and render a decision on the applicant's eligibility to occupy a sensitive position and have access to classified information.

c The applicant will receive a written decision from the WHS CAF through the Security Division.

(b) Post-Appointment (Employee)

(l) If unfavorable information involves a current employee, the WHS CAF will furnish the information to the Assistant Personnel Director, PSD, OA&IM, and refer the matter to the Employee Relations Division, PSD, OA&IM, for a suitability determination.

(2) If an unfavorable suitability determination is made, the Employee Relations Division will advise the WHS CAF and the Security Division of the determination and will initiate action to remove the employee.

(3) If an OIG, DoD, employee is determined suitable, the Employee Relations Division, PSD, OA&IM, will advise the WHS CAF, which will process the personnel security determination. If the WHS CAF determination is favorable, a security clearance will be issued and the Security Division notified. If the WHS CAF makes an unfavorable personnel security determination, the following actions will be taken:

a The WHS CAF will issue a SOR to the employee to deny or revoke the security clearance and eligibility for continued employment in a sensitive position. The SOR will be sent to the employee through the Security Division. The Security Division will prepare a memorandum of notice for suspension of access to classified and sensitive unclassified information. The WHS CAF SOR and the OIG, DoD, memorandum of notice will be presented to the employee by the applicable OIG Component Head and/or the supervisor.

1 The WHS CAF SOR, at a minimum, will:

aa Include a written statement of the reasons for the unfavorable personnel security action being taken.

bb Advise the employee of the right to reply to the WHS CAF SOR in writing and to provide documentary evidence and or affidavits in support of the reply.

cc Provide the employee with the investigative file used as the basis for the unfavorable determination.

dd Require the employee to notify the WHS CAF within 10 days of his/her intention to respond to the SOR.

ee Afford the employee 30 days, from the date of receipt, to reply to the SOR through the Security Division.

ff Provide the employee instructions for responding to the SOR (see Appendix D).

2 The employee's memorandum of notice will advise the employee of the following:

aa His/her access to classified and sensitive unclassified information and assignment to sensitive duties are suspended and will remain in a suspended status until a final determination is made by the WHS CAF.

bb He/she may respond to the Director, PSD, OA&IM, to the notice of suspension of access to classified and sensitive unclassified information within 7 days from the date of receipt of the memorandum.

cc An explanation of sensitive duties and sensitive unclassified information: "Duties and/or access requirements to any information that can be withheld from the public under the exemptions of the Freedom of Information Act, e.g., For Official Use Only (FOUO) and Privacy Act Information."

dd The requirement that the employee acknowledge receipt of the notice of suspension of access.

ee The requirement to return all classified and sensitive unclassified information to the supervisor.

ff The requirement to return OIG, DoD, credentials and courier authorization card to the Security Division.

gg The requirement that he/she read, sign and return to the Security Division an IG Form 5200.2-1, *Security Termination Statement*.

hh The termination of his/her access to the local area network (LAN).

3 The OIG Component Head’s memorandum of notice requests him/her to:

aa Ensure managers/supervisors at all levels suspend the employee's access to classified and/or sensitive unclassified information and assignment to sensitive duties.

bb Ensure action is taken to reassign the employee to non-sensitive duties. A "Statement of Differences" may be prepared and coordinated through the Employee Relations Division and the Operations Division, PSD, OA&IM.

cc Move the employee to another area to avoid inadvertent access to classified or sensitive unclassified information being processed within the work space.

dd Management may initiate through the Employee Relations Division, PSD, OA&IM, a proposed suspension from duty or reassignment of the employee to a vacant non-sensitive position. Alternatively, management has the option, but not an obligation, to restructure the position to remove all sensitive duties. The individual's access to classified and/or sensitive unclassified information will remain in a "suspended" status until a final determination is made by the WHS CAF.

b The SOR will be presented to the employee within 10 days through the OIG Component Head. The employee will be requested to sign the Acknowledgment of Receipt. A copy of the signed Acknowledgment and the employee's notice of intention to respond must be returned within 10 days to the WHS CAF through the Security Division to establish a 30-day suspense for the employee's response. If the employee refuses to sign the Acknowledgment, the supervisor will annotate the Receipt indicating the date and time of delivery and state that the employee refused to sign. The supervisor will sign his/her name below that statement.

c If the employee works outside the National Capital Region (NCR), the correspondence must be sent by registered mail to the employee through the OIG Component Head. A copy of the signed Acknowledgment of Receipt and the employee's notice of intention to respond must be returned within 10 days to the WHS CAF through the Security Division to establish a 30-day suspense for the employee's reply. If the employee refuses to sign the Acknowledgment, the supervisor will annotate the Receipt indicating the date and time of delivery and state that the employee refused to sign. The supervisor will sign his/her name below that statement.

d The Director, PSD, OA&IM, will inform the employee that he/she must return all classified and sensitive unclassified information, his/her OIG, DoD, credential, Courier Authorization Card and sign the IG Form 5200.2-1, *Security Termination Statement*. The employee will also be advised that action is underway to terminate his/her access to the LAN.

e The WHS CAF will consider all relevant information and render a decision on the employee's eligibility for continued employment in a sensitive position and access to classified and sensitive unclassified information. If the decision is favorable, the WHS CAF will issue a security clearance and advise the employee through the Security Division. The Security Division will take appropriate action to reinstate the employee's access to classified and sensitive unclassified information and to the LAN. If the decision is not favorable, the WHS CAF will issue a Letter of Denial/Revocation to the employee through the Security Division. The employee is advised that he/she may appeal the decision to the WHS CAB or to the Defense Office of Hearings and Appeals (DOHA), in accordance with Appendix E of this Regulation. The employee is required to notify the WHS CAF within 10 days of receipt of the Letter of Denial/Revocation of his/her intention to appeal the WHS CAF Letter of Denial/Revocation. The employee will also be advised that any appeal to the WHS CAB or the DOHA must be made within 30 days from the date of receipt.

f The employee may appeal to the WHS CAB in writing or in person to the DOHA and may provide documentary evidence and/or affidavits in support of the reply. The employee has the right to have a representative assist in the preparation and/or the presentation of the reply. However, the employee may not choose a representative that would result in a conflict of interest or position or with the priority needs of the OIG, DoD. The employee must make all arrangements for the representative and provide the name, address and telephone number of the representative to the WHS CAB or the DOHA through the Security Division. The WHS CAB or the DOHA will have the final authority to deny any representative because of conflict or priority needs of the OIG, DoD.

(4) The decision of the WHS CAB or the DOHA is final, and there is no further right to administrative review.

(5) If the final decision is favorable, a security clearance will be issued and the employee will be informed through the Security Division. If the final decision is unfavorable, management may initiate a proposed removal or reassignment of the employee to a vacant non-sensitive position. Alternatively, management has the option, but not an obligation, to restructure the position to remove all sensitive duties. Management must inform the Security Division, in writing, of the proposed action.

M. Personnel Security Clearances

1. Security clearances are issued by the WHS CAF after receipt of written notice from the OIG Component Head, through the Security Division based on the level of access required for the position.

2. When justified, the level of an individual's clearance can be upgraded by notifying the Security Division, in writing, of the need to do so. (The individual's clearance eligibility must be current and meet the required investigative standards.) Temporary upgrades of clearances will not normally affect position sensitivity unless temporary upgrades become frequent. Under those circumstances, the duties of the position should be reviewed by comparing them against the criteria listed in paragraph G of this Regulation. If the OIG Component Head determines the position sensitivity level should be upgraded, an SF 52 must be completed and forwarded to the Personnel Operations Division and the Security Division, PSD, OA&IM.

3. Clearances will not be granted under the following conditions:

(a) To persons in non-sensitive positions.

(b) To persons whose regular duties do not require access to classified and/or sensitive unclassified information.

(c) For ease of movement of personnel within a restricted, controlled or industrial area if duties do not require access to classified information and/or sensitive unclassified information.

(d) To persons who may only have inadvertent access to sensitive information or areas, such as guards, emergency service personnel, firemen, doctors, nurses, police, ambulance personnel or similar personnel.

(e) To persons who can be denied access to classified information by the presence of cleared personnel serving as escorts.

N. Continuing Security Responsibilities

1. A personnel security clearance is an assessment of an individual's trustworthiness for preserving and protecting national security. After a clearance is issued, there is a requirement for continuing that assessment.

2. Management officials should be able to identify any potential adverse security situations at an early stage and render any assistance required to preclude long-term, job-related security problems. Every supervisor and manager should become familiar with the "Criteria for Application of Security Standards" at Appendix B and the "Adjudicative Guidelines for Determining Eligibility for Access to Classified Information" at Appendix C of this Regulation. Managers must ensure that such matters are promptly reported to the Security Division, PSD, OA&IM, if and when they occur.

3. In addition to the items listed in Appendices B and C, each OIG, DoD, employee is required to report the following to the Security Division:

(a) All foreign travel (official and personal) in advance of departure.

(b) Any form of contact, intentional or otherwise, with individuals of any nationality, whether within or outside the scope of official activities when:

(1) Illegal or unauthorized access is sought to classified or otherwise sensitive information; or

(2) Concerns arise that he/she may be the target of exploitation by a foreign entity.

(c) Every OIG, DoD, employee is required to immediately notify his/her supervisor and the Security Division when he/she becomes aware of information with potentially serious security significance that could affect national security.

4. The Security Division will review the reported questionable/adverse information and if determined warranted, procedures to suspend the individual's access to classified and sensitive information will be initiated.

(a) A memorandum will be forwarded to the employee through the OIG component advising the employee of the tentative decision to suspend access and will:

(1) Advise the employee that he/she may respond to the Director, PSD, OA&IM, within 7 days from the date of receipt of the memorandum and provide mitigating circumstances. If the individual fails to respond and/or fails to provide any information to warrant a change to the proposed suspension of access decision, the adjudicative authority will be notified by the Security Division.

(2) Request the employee complete an SF 86.

(3) Request the return of all classified and sensitive unclassified material, credentials, courier authorization card and execute an IG Form 5200.2-1, *Security Termination Statement*. The employee's access to the LAN will be terminated.

(b) The adjudicative authority will be requested to enter the suspension of access into the DCII and to provide an adjudicative determination regarding the employee's continued eligibility for clearance and the occupancy of a sensitive position.

(c) The employee's access to classified and sensitive unclassified information will remain in a suspended status pending final resolution from the adjudicative authority.

(d) The OIG component will be directed to reassign the individual to non-sensitive duties.

O. Reinvestigations

1. Certain situations and requirements necessitate reinvestigation of an employee who has already been investigated. A reinvestigation is authorized as follows:

(a) To meet the periodic reinvestigation requirements of personnel assigned to special-sensitive or critical-sensitive positions and/or access to SCI, Top Secret or Secret information.

(b) To prove or disprove an allegation relating to the criteria contained in Appendices B and C of this Regulation.

(c) To assess the current eligibility of employees who previously were determined ineligible for access to classified information or who were determined eligible based on specified conditions.

2. The Security Division and/or the WHS CAF are responsible for requesting and processing all reinvestigations. Employees must execute forms required for initiation of the reinvestigation in the specified time allowed. Should the employee fail or refuse to execute the requested forms in the specified time, the Security Division will initiate action to tentatively suspend access to classified and/or sensitive unclassified information and occupancy of a sensitive position.

P. Security Education. The effectiveness of the OIG, DoD, Personnel Security Program is proportional to the degree employees understand their responsibilities within the program. An integral part of the program is security education. To ensure that personnel become aware of their responsibilities, security education training is provided through the following briefings:

1. **Initial Briefings**

(a) Personnel granted a security clearance are not permitted access to classified information until they are briefed on the requirements of safeguarding classified information and sign a "Classified Information Nondisclosure Agreement (NDA)." The PSD, OA&IM, will conduct the briefings for employees located within the NCR. The senior person in charge of OIG, DoD, field offices will ensure the briefings are conducted and documented. The completed NDA will be returned to the Security Division for filing in the employee's Official Personnel Folder. Refusal to sign the agreement will result in access denial and clearance revocation.

(b) Supervisors will personally brief new employees on their individual security responsibilities. The briefing will be tailored to meet the employee's specific job requirements and must be accomplished within 30 days of assignment.

(c) A mandatory security indoctrination will be provided by the Security Division for all incoming personnel assigned within the NCR. For personnel located outside the NCR, the senior person in charge will conduct the briefing. The pamphlet, IGDPH 5200.1, "Introduction to Security," contains an overview of security responsibilities and is available for distribution to all personnel.

2. **Refresher Briefings.** The Security Division conducts annual refresher briefings for personnel in the NCR. The senior person in charge of OIG field offices will conduct the briefings for field personnel and forward certificates of completion to the Security Division. This training reacquaints the employee with his/her responsibilities on the various requirements for handling classified information and other elements of the Personnel Security Program.

3. **Foreign Travel Briefings.** The OIG, DoD, personnel are required to report all foreign travel to the Security Division. A Foreign Travel Briefing may be required under some circumstances.

4. **Termination Briefings**

(a) Military personnel and civilian employees receive a termination briefing when:

(1) Assignment and/or employment is terminated.

(2) A contemplated absence from duty or employment will last for 60 days or more.

(3) Access to classified and/or sensitive unclassified information is suspended.

(b) When any of those reasons apply, employees assigned within the NCR must report to the Security Division to sign an IG Form 5200.2-1, *Security Termination Statement*. The senior person in charge of OIG, DoD, field offices will ensure the briefings are conducted and documented. The senior person in charge will ensure that the completed form is returned to the Security Division.

(c) If an employee refuses to execute a Security Termination Statement, an oral debriefing will be given in the presence of a witness and documented on the IG Form 5200.2-1. The briefer and witness will sign beneath the statement attesting to the action, and the completed form will be forwarded to the Security Division. The refusal to sign a Security Termination Statement will be recorded in the DCII.

(d) Security Termination Statements will be retained by the Security Division for 2 years.

Q. Effective Date of Implementation. This Regulation is effective immediately.

FOR THE INSPECTOR GENERAL:

//Signed//
Joel L. Leson
Director
Administration and
Information Management

5 Appendices - a/s

APPENDIX A
REFERENCES

a. DoD Regulation 5200.2-R, "Department of Defense Personnel Security Program," January 1987, Change 1, 2, 3

b. Federal Personnel Manual, Chapter 731, "Personnel Suitability" and Chapter 732, "Personnel Security"

c. DoD 5200.1-R, “DoD Information Security Program Regulation,” January 1997

d. Section 552a, title 5, United States Code

e. Executive Order 12968, "Access to Classified Information," August 2, 1995

f. DoD Directive 5200.2, “DoD Personnel Security Program,” April 9, 1999

g. Executive Order 12958, “Classified National Security Information,” April 17, 1995

h. Section 781, title 50, United States Code

i. Section 831 through 835, title 50, United States Code

j. DoD Directive 5200.28, "Security Requirements for Automated Information Systems," March 21, 1988

k. Executive Order 10450, "Security Requirements for Government Employment," April 21, 1953

l. Title 2, United States Code, “Comprehensive Drug Abuse Prevention and Control Act of 1970”

APPENDIX B
CRITERIA FOR APPLICATION OF SECURITY STANDARDS
(As extracted from DoD Regulation 5200.2-R)

a. Commission of any act of sabotage, espionage, treason, terrorism, anarchy, sedition or attempts thereat or preparation therefor, or conspiring with or aiding or abetting another to commit or attempt to commit any such act.

b. Establishing or continuing a sympathetic association with a saboteur, spy, traitor, seditionist, anarchist, terrorist, revolutionist or with an espionage or other secret agent or similar representative of a foreign nation whose interests may be contrary to the interests of the United States, or with any person who advocates the use of force or violence to overthrow the Government of the United States or to alter the form of Government of the United States by unconstitutional means.

c. Advocacy or use of force or violence to overthrow the Government of the United States or to alter the form of Government of the United States by unconstitutional means.

d. Knowing membership with the specific intent of furthering the aims of, or adherence to and active participation in, any foreign or domestic organization, association, movement, group or combination of persons (hereafter referred to as organizations) that unlawfully advocate or practice the commission of acts of force or violence to prevent others from exercising their rights under the Constitution or laws of the United States or of any state or which seek to overthrow the Government of the United States or any state or subdivision thereof by unlawful means.

e. Unauthorized disclosure to any person of classified information or other information, the disclosure of which is prohibited by statute, executive order or regulation.

f. Performing or attempting to perform one's duties, acceptance and active maintenance of dual citizenship, or other acts conducted in a manner that serve or could be expected to serve the interests of another government in preference to the interests of the United States.

g. Disregard of public law, statutes, executive orders or regulations, including violation of security regulations or practices.

h. Criminal or dishonest conduct.

i. Acts of omission or commission that indicate poor judgment, unreliability or untrustworthiness.

j. Any behavior or illness, including any mental condition, which, in the opinion of competent medical authority, may cause a defect in judgment or reliability with due regard to the transient or continuing effect of the illness and the medical findings in such a case.

k. Vulnerability to coercion, influence or pressure that may cause conduct contrary to the national interest. This may be (1) the presence of immediate family members or other persons to whom the applicant is bonded by affection or obligation in a nation (or areas under its domination) whose interests may be inimical to those of the United States, or (2) any other circumstances that could cause the applicant to be vulnerable.

l. Excessive indebtedness, recurring financial difficulties or unexplained affluence.

m. Habitual or episodic use of intoxicants to excess.

n. Illegal or improper use, possession, transfer, sale or addiction to any controlled or psychoactive substance, narcotic, cannabis or other dangerous drug.

o. Any knowing and willful falsification, cover-up, concealment, misrepresentation or omission of a material fact from any written or oral statement, document, form or other representation or device used by the DoD or any other Federal agency.

p. Failing or refusing to answer or to authorize others to answer questions or provide information required by a congressional committee, court or agency in the course of an official inquiry whenever such answers or information concern relevant and material matters pertinent to an evaluation of the individual's trustworthiness, reliability and judgment.

q. Acts of sexual misconduct or perversion indicative of moral turpitude, poor judgment or lack of regard for the laws of society.

APPENDIX C
ADJUDICATIVE GUIDELINES FOR DETERMINING ELIGIBILITY FOR ACCESS TO CLASSIFIED INFORMATION

A. Purpose. The following adjudicative guidelines are established for all U.S. Government civilian and military personnel, consultants, contractors, employees of contractors, licensees, certificate holders or grantees and their employees and other individuals who require access to classified information. They apply to persons being considered for initial or continued eligibility for access to classified information, to include sensitive compartmented information and special access programs, and are to be used by Government departments and agencies in all final clearance determinations.

B. Adjudicative Process

1. The adjudicative process is an examination of a sufficient period of a person's life to make an affirmative determination that the person is an acceptable security risk. Eligibility for access to classified information is predicated upon the individual meeting these personnel security guidelines. The adjudication process is the careful weighing of a number of variables known as the whole person concept. All available, reliable information about the person, past and present, favorable and unfavorable, should be considered in reaching a determination. In evaluating the relevance of an individual's conduct, the adjudicator should consider the following factors:

(a) The nature extent, and seriousness of the conduct.

(b) The circumstances surrounding the conduct, to include knowledgeable participation.

(c) The frequency and recency of the conduct.

(d) The individual's age and maturity at the time of the conduct.

(e) Whether or not participation was voluntary.

(f) The presence or absence of rehabilitation and other pertinent behavioral changes.

(g) The motivation for the conduct.

(h) The potential for pressure, coercion, exploitation or duress.

(i) The likelihood of continuation or recurrence.

2. Each case must be judged on its own merits and final determination remains the responsibility of the specific department or agency. Any doubt concerning a person’s consideration for access to classified information will be resolved in favor of national security and considered final.

3. The ultimate determination of whether to grant or continue eligibility for a security clearance is clearly consistent with the interests of national security and must be an overall common sense determination based upon careful consideration of the following:

(a) Allegiance to the United States

(b) Foreign influence

(c) Foreign preference

(d) Sexual behavior

(e) Personal conduct

(f) Financial considerations

(g) Alcohol consumption

(h) Drug involvement

(i) Emotional, mental and personality disorders

(j) Criminal conduct

(k) Security violations

(l) Outside activities

(m) Misuse of information technology systems

4. Each of the foregoing should be evaluated in the context of the whole person.

5. Although adverse information concerning a single criterion may not be sufficient for an unfavorable determination, the individual may be disqualified if available information reflects a recent or recurring pattern of questionable judgment, irresponsibility or emotionally unstable behavior.

6. However, notwithstanding the whole person concept, pursuit of further investigation may be terminated by an appropriate adjudicative agency in the face of reliable, significant, disqualifying, adverse information.

7. When information of security concern becomes known about an individual who is currently eligible for access to classified information, the adjudicator should consider whether the person:

(a) Voluntarily reported the information.

(b) Sought assistance and followed professional guidance, where appropriate.

(c) Resolved or appears likely to favorably resolve the security concern.

(d) Has demonstrated positive changes in behavior and employment.

(e) Should have his or her access temporarily suspended pending final adjudication of the information.

8. If, after evaluating information of security concern, the adjudicator decides that the information is not serious enough to warrant a recommendation of disapproval or revocation of the security clearance, it may be appropriate to recommend approval with a warning that future incidents of a similar nature may result in revocation of access.

9. The information at the beginning of each adjudicative guideline provides a brief explanation of its relevance in determining whether it is clearly consistent with the interest of national security to grant or continue a person's eligibility for access to classified information.

ALLEGIANCE TO THE UNITED STATES

An individual must be of unquestioned allegiance to the United States. The willingness to safeguard classified information is in doubt if there is any reason to suspect an individual's allegiance to the United States.

Conditions that could raise a security concern and may be disqualifying include:

(1) Involvement in any act of sabotage, espionage, treason, terrorism, sedition or other act whose aim is to overthrow the Government of the United States or alter the form of government by unconstitutional means.

(2) Association or sympathy with persons who are attempting to commit, or who are committing, any of the above acts.

(3) Association or sympathy with persons or organizations that advocate the overthrow of the United States Government, or any state or subdivision, by force or violence or by other unconstitutional means.

(4) Involvement in activities that unlawfully advocate or practice the commission of acts of force or violence to prevent others from exercising their rights under the Constitution or laws of the United States or of any state.

Conditions that could mitigate security concerns include:

(1) The individual was unaware of the unlawful aims of the individual or organization and severed ties upon learning of those aims.

(2) The individual's involvement was only with the lawful or humanitarian aspects of such an organization.

(3) Involvement in the above activities occurred for only a short period of time and was attributable to curiosity or academic interest.

(4) The person has had no recent prescribed involvement or association with such activities.

FOREIGN INFLUENCE

A security risk may arise when an individual's immediate family, including cohabitants, and other persons to whom he or she may be bound by affection, influence or obligation are: (1) not citizens of the United States or (2) may be subject to duress. These situations could create the potential for foreign influence that could result in the compromise of classified information. Contacts with citizens of other countries or financial interests in other countries are also relevant to security determinations if they make an individual potentially vulnerable to coercion, exploitation or pressure.

Conditions that could raise a security concern and may be disqualifying include:

(1) An immediate family member, or a person to whom the individual has close ties of affection or obligation, is a citizen of, or resident or present in, a foreign country.

(2) Sharing living quarters with a person or persons, regardless of their citizenship status, if the potential for adverse foreign influence or duress exists.

(3) Relatives, cohabitants or associates who are connected with any foreign government.

(4) Failing to report, where required, associations with foreign nationals.

(5) Unauthorized association with a suspected or known collaborator or employee of a foreign intelligence service.

(6) Conduct that may make the individual vulnerable to coercion, exploitation or pressure by a foreign government.

(7) Indications that representatives or nationals from a foreign country are acting to increase the vulnerability of the individual to possible future exploitation, coercion or pressure.

(8) A substantial financial interest in a country or in any foreign owned or operated business that could make the individual vulnerable to foreign influence.

Conditions that could mitigate security concerns include:

(1) A determination that the immediate family member(s), cohabitant, or associate(s) in question would not constitute an unacceptable security risk.

(2) Contacts with foreign citizens are the result of official U.S. Government business.

(3) Contact and correspondence with foreign citizens are casual and infrequent.

(4) The individual has promptly reported to proper authorities all contacts, requests or threats from persons or organizations from a foreign country, as required.

(5) Foreign financial interests are minimal and not sufficient to affect the individual's security responsibilities.

FOREIGN PREFERENCE

When an individual acts in such a way as to indicate a preference for a foreign country over the United States, then he or she may be prone to provide information or make decisions that are harmful to the interests of the United States.

Conditions that could raise a security concern and may be disqualifying include:

(1) The exercise of dual citizenship.

(2) Possession and/or use of a foreign passport.

(3) Military service or a willingness to bear arms for a foreign country.

(4) Accepting educational, medical or other benefits, such as retirement and social welfare, from a foreign country.

(5) Residence in a foreign country to meet citizenship requirements.

(6) Using foreign citizenship to protect financial or business interests in another country.

(7) Seeking or holding political office in the foreign country.

(8) Voting in foreign elections.

(9) Performing or attempting to perform duties, or otherwise acting, so as to serve the interests of another government in preference to the interests of the United States.

Conditions that could mitigate security concerns include:

(1) Dual citizenship is based solely on parents' citizenship or birth in a foreign country.

(2) Indicators of possible foreign preference (e.g., foreign military service) occurred before obtaining United States citizenship.

(3) Activity is sanctioned by the United States.

(4) The individual has expressed a willingness to renounce dual citizenship.

SEXUAL BEHAVIOR

Sexual behavior is a security concern if it involves a criminal offense, indicates a personality or emotional disorder, subjects the individual to undue influence or coercion or reflects a lack of judgment or discretion.[1] (Sexual orientation or preference may not be used as a basis for, or a disqualifying factor in, determining a person's eligibility for a security clearance.)

Conditions that could raise a security concern and may be disqualifying include:

(1) Sexual behavior of a criminal nature, whether or not the individual has been prosecuted.

(2) Compulsive or addictive sexual behavior when the person is unable to stop a pattern of self-destructive or high-risk behavior or that which is symptomatic of a personality disorder.

(3) Sexual behavior that causes an individual to be vulnerable to undue influence or coercion.

(4) Sexual behavior of a public nature and/or that which reflects a lack of discretion or judgment.

Conditions that could mitigate security concerns include:

(1) The behavior occurred during or before adolescence, and there is no evidence of subsequent conduct of a similar nature.

(2) The behavior was not recent, and there is no evidence of subsequent conduct of a similar nature.

(3) There is no other evidence of questionable judgment, irresponsibility or emotional instability.

(4) The behavior no longer serves as a basis for undue influence or coercion.

[1]The adjudicator should also consider guidelines pertaining to criminal conduct or emotional, mental and personality disorders in determining how to resolve the security concerns raised by sexual behavior.

PERSONAL CONDUCT

Conduct involving questionable judgment, untrustworthiness, unreliability or unwillingness to comply with rules and regulations could indicate that the person may not properly safeguard classified information.

The following will normally result in an unfavorable clearance action or administrative termination of further processing for clearance eligibility:

(1) Refusal to undergo or cooperate with required security processing, including medical and psychological testing.

(2) Refusal to complete required security forms, releases or provide full, frank and truthful answers to lawful questions of investigators, security officials or other official representatives in connection with a personnel security or trustworthiness determination.

Conditions that could raise a security concern and may be disqualifying also include:

(1) Reliable, unfavorable information provided by associates, employers, coworkers, neighbors and other acquaintances.

(2) The deliberate omission, concealment or falsification of relevant and material facts from any personnel security questionnaire, personal history statement or similar form used to conduct investigations, determine employment qualifications, award benefits or status, determine security clearance eligibility or trustworthiness or award fiduciary responsibilities.

(3) Deliberately providing false or misleading information concerning relevant and material matters to an investigator, security official, competent medical authority or other official representative in connection with a personnel security or trustworthiness determination.

(4) Personal conduct or concealment of information that increases an individual's vulnerability to coercion, exploitation or pressure.

(5) A pattern of dishonesty or rule violations[2].

(6) Association with persons involved in criminal activity.

Conditions that could mitigate security concerns include:

(1) The information was unsubstantiated or not pertinent to a determination of judgment, trustworthiness or reliability.

(2) The falsification was an isolated incident, was not recent and the individual has subsequently provided correct information voluntarily.

(3) The individual made prompt, good faith efforts to correct the falsification before being confronted with the facts.

[2]To include violation of any written or recorded agreement made between the employee and the agency.

(4) Omission of material facts was caused or significantly contributed to by improper or inadequate advice of authorized personnel, and the previously oriented information was promptly and fully provided.

(5) The individual has taken positive steps to significantly reduce or eliminate vulnerability to coercion, exploitation or pressure.

(6) A refusal to cooperate was based on advice from legal counsel or other officials that the individual was not required to comply with security processing requirements and, upon being made aware of the requirement, fully and truthfully provided the requested information.

(7) Association with persons involved in criminal activities has ceased.

FINANCIAL CONSIDERATIONS

An individual who is financially overextended is at risk of having to engage in illegal acts to generate funds. Unexplained affluence is often linked to proceeds from financially profitable criminal acts.

Conditions that could raise a security concern and may be disqualifying include:

(1) A history of not meeting financial obligations.

(2) Deceptive or illegal financial practices such as embezzlement, employee theft, check fraud, income tax evasion, expense account fraud, filing deceptive loan statements and other intentional financial breaches of trust.

(3) Inability or unwillingness to satisfy debts.

(4) Unexplained affluence.

(5) Financial problems that are linked to gambling, drug abuse, alcoholism or other issues of security concern.

Conditions that could mitigate security concerns include:

(1) The behavior was not recent.

(2) It was an isolated incident.

(3) The conditions that resulted in the behavior were largely beyond the person's control (e.g., loss of employment, a business downturn, unexpected medical emergency or a death, divorce or separation).

(4) The person has received or is receiving counseling for the problem, and there are clear indications that the problem is being resolved or is under control.

(5) The affluence resulted from a legal source.

(6) The employee initiated a good faith effort to repay overdue creditors or otherwise resolve debts.

ALCOHOL CONSUMPTION

Excessive alcohol consumption often leads to the exercise of questionable judgment, unreliability, failure to control impulses and increases the risk of unauthorized disclosure of classified information due to carelessness.

Conditions that could raise a security concern and may be disqualifying include:

(1) Alcohol-related incidents away from work, such as driving while under the influence, fighting, child or spouse abuse or other criminal incidents related to alcohol use.

(2) Alcohol-related incidents at work, such as reporting for work or duty in an intoxicated or impaired condition or drinking on the job.

(3) Diagnosis by a credentialed medical professional[3] of alcohol abuse or alcohol dependence.

(4) Habitual or binge consumption of alcohol to the point of impaired judgment.

(5) Consumption of alcohol, subsequent to a diagnosis of alcoholism by a credentialed medical professional and following completion of an alcohol rehabilitation program.

Conditions that could mitigate security concerns include:

(1) The alcohol related incidents do not indicate a pattern.

(2) The problem occurred a number of years ago, and there is no indication of a recent problem.

(3) Positive changes in behavior that are supportive of sobriety.

(4) Following diagnosis of alcohol abuse or alcohol dependence, the individual has successfully completed inpatient or outpatient rehabilitation, along with aftercare requirements; participates frequently in meetings of Alcoholics Anonymous or a similar organization; abstained from alcohol for a period of at least 12 months; and received a favorable prognosis by a credentialed medical professional.

[3]Credentialed medical professional: licensed physician, licensed clinical psychologist or board certified psychiatrist.

DRUG INVOLVEMENT

Improper or illegal involvement with drugs raises questions regarding an individual's willingness or ability to protect classified information. Drug abuse or dependence may impair social or occupational functioning, increasing the risk of an unauthorized disclosure of classified information.

Drugs are defined as mood and behavior altering:

(1) Drugs, materials and other chemical compounds identified and listed in the Comprehensive Drug Abuse Prevention and Control Act of 1970 (e.g., marijuana or cannabis, depressants, narcotics, stimulants and hallucinogens) (reference l).

(2) Inhalants and other similar substances.

Drug abuse is the illegal use of a drug or use of a legal drug in a manner that deviates from approved medical direction.

Conditions that could raise a security concern and may be disqualifying include:

(1) Any drug abuse (see above definitions).

(2) Illegal drug possession, including cultivation, processing, manufacture, purchase, sale or distribution.

(3) Failure to successfully complete a drug treatment program prescribed by a credentialed medical professional.[4] Current drug involvement, especially following the granting of a security clearance, or an expressed intent not to discontinue use, will normally result in an unfavorable determination.

Conditions that could mitigate security concerns include:

(1) The drug involvement was not recent.

(2) The drug involvement was an isolated or infrequent event.

(3) A demonstrated intent not to abuse any drugs in the future.

(4) Satisfactory completion of a drug treatment program prescribed by a credentialed medical professional.

[4]Credentialed medical professional: licensed physician, licensed clinical psychologist or board certified psychiatrist.

EMOTIONAL, MENTAL AND PERSONALITY DISORDERS

Emotional, mental and personality disorders can cause a significant deficit in an individual's psychological, social and occupational functioning. Those disorders are of security concern because they may indicate a defect in judgment, reliability or stability.

When appropriate, a credentialed mental health professional,[5] acceptable to or approved by the Government, should be consulted so that potentially disqualifying and mitigating information may be fully and properly evaluated.

Conditions that could raise a security concern and may be disqualifying include:

(1) A diagnosis by a credentialed mental health professional that the individual has a disorder that could result in a defect in psychological, social or occupational functioning.

(2) Information that suggests an employee has failed to follow appropriate medical advice relating to treatment of a diagnosed disorder, e.g., failure to take prescribed medication.

(3) A pattern of high-risk, irresponsible, aggressive, anti-social or emotionally unstable behavior.

(4) Information that suggests the employee's current behavior indicates a defect in his/her judgment or reliability.

Conditions that could mitigate security concerns include:

(1) There is no indication of a current problem.

(2) Recent diagnosis by a credentialed mental health professional that an employee's previous emotional, mental or personality disorder is cured or in remission and has a low probability of recurrence or exacerbation.

(3) The past emotional instability was a temporary condition (e.g., one caused by a death, illness or marital breakup), the situation has been resolved and the individual is no longer emotionally unstable.

[5]Credentialed mental health professional: licensed clinical psychologist, licensed social worker or board certified psychiatrist.

CRIMINAL CONDUCT

A history or pattern of criminal activity creates doubt about a person's judgment, reliability and trustworthiness.

Conditions that could raise a security concern and may be disqualifying include:

(1) Any criminal conduct, regardless of whether the person was formally charged.

(2) A single serious crime or multiple lesser offenses.

Conditions that could mitigate security concerns include:

(1) The criminal behavior was not recent.

(2) The crime was an isolated incident.

(3) The person was pressured or coerced into committing the act, and those pressures are no longer present in that person's life.

(4) The person did not voluntarily commit the act, and/or the factors leading to the violation are not likely to recur.

(5) There is clear evidence of successful rehabilitation.

SECURITY VIOLATIONS

Noncompliance with security regulations raises doubt about an individual's trustworthiness, willingness and ability to safeguard classified information.

Conditions that could raise a security concern and may be disqualifying include:

(1) Unauthorized disclosure of classified information.

(2) Violations that are deliberate or multiple or due to negligence.

Conditions that could mitigate security concerns include actions that:

(1) Were inadvertent.

(2) Were isolated or infrequent.

(3) Were due to improper or inadequate training.

(4) Demonstrate a positive attitude towards the discharge of security responsibilities.

OUTSIDE ACTIVITIES

Involvement in certain types of outside employment or activities is of security concern if it poses a conflict with an individual's security responsibilities and could create an increased risk of unauthorized disclosure of classified information.

Conditions that could raise a security concern and may be disqualifying include any service, whether compensated, volunteer or employment with:

(1) A foreign country.

(2) Any foreign national.

(3) A representative of any foreign interest.

(4) Any foreign, domestic or international organization or person engaged in analysis, discussion or publication of material on intelligence, defense, foreign affairs or protected technology.

Conditions that could mitigate security concerns include:

(1) Evaluation of the outside employment or activity indicates that it does not pose a conflict with an individual's security responsibilities.

(2) The individual terminates the employment or discontinues the activity when notified that it is in conflict with his or her security responsibilities.

MISUSE OF INFORMATION TECHNOLOGY SYSTEMS

Noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems may raise security concerns about an individual's trustworthiness, willingness and ability to properly protect classified systems, networks and information.

Information technology systems include all related equipment used for the communication, transmission, processing, manipulation and storage of classified or sensitive information.

Conditions that could raise a security concern and may be disqualifying include:

(1) Illegal or unauthorized entry into any information technology system.

(2) Illegal or unauthorized modification, destruction, manipulation or denial of access to information residing on an information technology system.

(3) Removal (or use) of hardware, software or media from any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations.

(4) The use of non-standard hardware or software is an OIG component-level management decision. The Information Systems Directorate (ISD), OA&IM, shall not support microcomputer hardware or software that the Chief Information Officer (CIO) has not declared an OIG, DoD, standard. Any OIG component that chooses to use non-standard microcomputer hardware or software is responsible for the functioning of those information resources. That includes any effect that microcomputer hardware or software may have on the operation of standard microcomputer hardware and software. Even virus-free information resources may cause conflicts when introduced into the OIG, DoD, environment. If the ISD, OA&IM, determines that introduced microcomputer hardware or software are causing malfunction of standard microcomputer hardware or software, the ISD, OA&IM, will return the user to the standard configuration. The ISD, OA&IM, will not assume responsibility for any functionality or data lost by return to the standard configuration. Any exceptions to this provision must be negotiated between the OIG component and the ISD, OA&IM.

Conditions that could mitigate security concerns include:

(1) The misuse was not recent or significant.

(2) The conduct was unintentional or inadvertent.

(3) The introduction or removal of media was authorized.

(4) The misuse was an isolated event.

(5) The misuse was followed immediately by a prompt, good faith effort to correct the situation.

APPENDIX D
INSTRUCTIONS FOR RESPONDING TO A STATEMENT OF REASONS

A. These instructions are intended to provide guidance in responding to the Washington Headquarters Services Consolidated Adjudication Facility (WHS CAF) preliminary decision to deny or revoke an employee's eligibility for access to classified information or employment in sensitive duties.

B. It is in the best interest of the employee to provide the most complete and accurate information possible during this preliminary stage of the decision-making process. Therefore, if the individual decides to challenge the preliminary decision, he/she must respond to the WHS CAF Statement of Reasons (SOR) and provide any other information that should be considered by the WHS CAF in making a final decision.

C. This preliminary decision will automatically become final if the employee fails to notify the WHS CAF within 10 days that he/she intends to respond to the SOR. The employee will also lose the right to appeal the final decision if he/she does not submit a timely response. If the decision becomes final, the employee will not be eligible to handle classified information or perform sensitive duties. That could prevent the individual from continuing in his/her present sensitive position and/or future employment with sensitive duties within the DoD.

D. The SOR is based on adverse information revealed by an investigation of the employee's personal history. Specific security concerns about the employee's conduct or background, along with supporting adverse information, are provided in the WHS CAF SOR.

1. **Before Responding**

a. **Follow the instructions**. The SOR and these instructions provide specific requirements and deadlines for compliance. The employee will forfeit the right to appeal if he/she fails to follow the instructions. He/she must notify the WHS CAF via the Security Division, PSD, OA&IM, within 10 days as to whether or not he/she intends to respond. If the employee chooses to respond, the response must be submitted to the Security Division, PSD, OA&IM, within 30 days from the date the SOR is received.

b. **Review adverse information**. The employee should carefully read the security concerns and supporting adverse information included in the SOR. Determine whether the findings are accurate and whether circumstances are not included that might have a favorable bearing on the case.

c. **Obtain and organize supporting documents**. The employee should provide any documentation that supports his/her case. The documentation should be organized according to the security concerns presented. The most useful documents will be those that refute, correct, explain, extenuate, mitigate or update the adverse information. Examples of useful documentation include copies of correspondence, court records with details or dispositions of arrests and status of probation; receipts; copies of canceled checks or letters from creditors verifying the status of delinquent accounts; certificates of completion for rehabilitation programs; releases from judgment or attachment; transcripts of court testimony taken under oath; probation reports; copies of negotiated plea bargains; etc. Mere statements, such as "I paid those bills," "I didn't do it" or "It wasn't my fault" will not carry as much weight as supporting documentation. The employee may provide statements from his/her supervisor, co-workers and/or others concerning the employee's judgment, reliability and trustworthiness, and any other information that should be considered before a final decision is made.

d. **Seek assistance**. The Security Division, PSD, OA&IM, has been designated as the point of contact with the WHS CAF. Employees may obtain legal counsel or other assistance in preparing responses. However, if the employee obtains assistance, the employee is responsible for all expenses incurred.

2. **Writing a Response**

a. All responses should be in the form of a letter from the employee to the WHS CAF through the Security Division, PSD, OA&IM. The employee is required to address each security concern and/or each item of supporting adverse information separately.

b. It is essential that each security concern and its supporting adverse information is addressed. Information that explains, refutes, corrects, extenuates, mitigates or updates each security concern must be provided. The employee should include, wherever possible, copies of the types of documents described above. The response should be organized with supporting documents enclosed in the order they are referred to in the SOR.

c. The impact of the employee's response will depend on the extent to which he/she can specifically refute, correct, extenuate, mitigate or update security concerns and adverse information. Information that is untrue should be specifically refuted. If the employee believes that the adverse information, though true, does not support the security concern or presents an incomplete picture, he/she should provide information that explains his/her case or lessens and/or disproves the security concern.

d. Personnel security guidelines are used by the WHS CAF to determine whether certain adverse information is of a security concern. The guidelines pertinent to the specific security concern of the WHS CAF will be included as an enclosure to the SOR. The guidelines are used by the WHS CAF in determining whether an individual should be granted eligibility for access to classified information or permitted to performing sensitive duties. The guidelines provide a framework for weighing all available information, both favorable information as well as adverse information, that is of security concern.

e. The employee's written response and supporting documents should be placed in a single envelope or package and forwarded to the WHS CAF via the Security Division, PSD, OA&IM, within the time allowed. The employee will be notified in writing of the WHS CAF final decision, and in most cases the decision will be made within 60 days. If the decision is favorable, the employee's access eligibility will be granted or restored. If not, the employee may appeal the decision to the higher authority, the Washington Headquarters Clearance Appeals Board (WHS CAB) or the Defense Office of Hearings and Appeals (DOHA).

APPENDIX E
INSTRUCTIONS FOR APPEALING A LETTER OF DENIAL/REVOCATION

A. These instructions are intended to provide guidance in responding to the Washington Headquarters Services Consolidated Adjudication Facility (WHS CAF) final decision to deny or revoke an employee's eligibility for access to classified information or employment in sensitive duties.

B. The WHS CAF letter of denial or revocation (LOD) explains the final decision. The LOD is based on adverse information that raises security concerns about the employee's trustworthiness, reliability or judgment.

1. **How to Appeal.** The LOD can be appealed in one of two ways:

a. The employee may request a personal appearance before an administrative judge (AJ) from the Defense Office of Hearings and Appeals (DOHA). That appearance is intended to provide the employee with an additional opportunity to present a full picture of his/her situation. The employee will have an opportunity to orally respond to the security concerns noted in the LOD and submit supporting documentation to the AJ, who will make a recommendation to the WHS CAB. The WHS CAB will consider both a written record and the results of the personal appearance in making its final decision.

b. The employee may, however, prefer to submit a written appeal to the WHS CAB and forego the personal appearance. If the employee submits a written appeal, he/she may also provide supporting documentation.

c. The employee must elect either (a) or (b) as stated above; the employee may not do both.

2. **Appealing with a Personal Appearance**

a. An employee appealing an LOD may request a personal appearance by writing to the DOHA at the following address: Director, Defense Office of Hearings and Appeals, Post Office Box 3656, Arlington, Virginia 22203 (Telefax No. 703-696-6865). The request must be sent through the Security Division, PSD, OA&IM, to the DOHA within 10 days of receipt of the LOD. An extension of time may be granted by the Director, DOHA, or designee for good cause demonstrated by the appellant.

b. Upon receipt of a request for a personal appearance, the DOHA shall promptly request the appellant's case file from the appropriate WHS CAF, assign the case to an AJ and provide a copy of the request to the WHS CAB. The WHS CAF shall provide the case file to the DOHA normally within 10 days.

c. The AJ will schedule a personal appearance generally within 30 days from receipt of the request and arrange for a verbatim transcript of the proceeding. For appellants at duty stations within the Continental United States, the personal appearance will be conducted at the appellant's duty station or a nearby suitable location. For individuals assigned to duty stations outside the Continental United States, the personal appearance will be conducted at the appellant's duty station or a nearby suitable location, or at DOHA facilities located in the Washington, D.C. metropolitan area or the Los Angeles, California, metropolitan area as determined by the Director, DOHA, or designee.

d. Travel costs for the appellant will be the responsibility of the employing organization.

e. In preparing for the personal appearance, the employee should ensure that he/she is able to address all of the security concerns and supporting adverse information. The supporting documents should be organized and readily accessible for presentation to the AJ presiding at the appearance and for use in answering questions.

f. The AJ presiding at the appearance will have already reviewed the employee's case file. Therefore, the employee's goal should be to clarify his/her reasons for overturning the LOD and adding additional information and documentation when appropriate rather than merely to repeat material previously submitted. The employee will not have the opportunity to present or cross-examine witnesses. If the employee wants the views of others presented, the employee should make sure that he/she obtains those views in writing (e.g., letters of reference, letters from medical authorities, etc.) and that he/she presents the documents to the AJ.

g. At the appearance, the employee will have an opportunity to present oral and documentary information on his/her own behalf. The personal appearance is designed so that the employee can represent himself/herself; he/she may obtain legal counsel or other assistance at his/her own expense to be present at the appearance. Postponement of the personal appearance can be granted only for good cause.

h. During the appearance, the employee is allowed to make an oral presentation and submit documentation. The employee may be asked questions, and the answers should be clear, complete and honest. The AJ will not present the Government's security concerns but rather will listen to any explanations the employee may have concerning his/her case.

i. At the end of the personal appearance, the employee will be given an opportunity to make a closing statement. The closing statement should highlight how the weight of all available information supports overturning the unfavorable personnel security determination in the case.

j. Upon completion of the personal appearance, the AJ will generally forward within 30 days a written recommendation to the appropriate WHS CAB whether to sustain or overturn the LOD, along with the case file and any documents submitted by the appellant. A copy of the AJ's recommendation will be provided to the WHS CAF.

k. The WHS CAB will render a final written determination stating its rationale and notify the employee in writing (via the employee's organization) generally within 30 days of receipt of the recommendation from the DOHA. That decision will be final and will conclude the appeal process.

4. **Appealing Without a Personal Appearance**

a. If the employee chooses to appeal without a personal appearance, a written response should provide whatever information the employee wants considered in the final decision. The employee should try to specifically explain, refute, extenuate, mitigate or update the security concerns presented in the LOD.

b. The employee should review the "Instructions for Responding to a Statement of Reasons" (Appendix B of this Regulation) to ensure that the appeal follows the guidelines outlined in that document. The Instructions will provide an understanding of how to develop and write the appeal to address the security concerns of the WHS CAF. The employee should provide any supporting documents in his/her case. The documentation should be organized in the order that the security concerns are presented.

c. The individual should place the written appeal and supporting documents in a single envelope or package and forward it to the WHS CAB via the Security Division, PSD, OA&IM, within the time allowed.